IN THE CLAIMS:

Please **CANCEL** claims 2-3 and 15-16 without prejudice or disclaimer.

Please **AMEND** claims 1, 5-6, 14, 17-24, and 28 as shown below.

1. (Currently Amended) A method of generating a subscriber identifier, the method comprising:

generating an identifier base string based on encrypting a subscriber identifying value;

generating an integrity check value based on the identifier base string; and

generating the subscriber identifier based on a concatenation of the identifier base string and the integrity check value.

wherein the generating the identifier base string comprises:

binary coding of the subscriber identifying value,

concatenating a random number, and

performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string.

2. (Cancelled)

3. (Cancelled)

4. (Previously Presented) The method according to claim 1, further comprising:

using a key indicator for indicating a used ciphering key,

wherein the generating the identifier base string comprises concatenating the key indicator to a value obtained by the encryption of the subscriber identifying value.

5. (Currently Amended) The method according to claim ~~2~~1, further comprising:

using an identifier type indicator for indicating that the subscriber identifier is a particular identifier type,

wherein the generating the identifier base string comprises concatenating the identifier type indicator to a value obtained by the encryption of the subscriber identifying value.

6. (Currently Amended) The method according to claim ~~2~~1, wherein the performing the encryption algorithm comprises providing a defined length for the concatenated binary coded subscriber identifying value and the random number, wherein most significant bits not used for the binary coded subscriber identifying value are set to 1, respectively.

7. (Original) The method according to claim 1, wherein the integrity check value is generated by performing a pseudo random function on the identifier base string using an integrity key.

8. (Previously Presented) The method according to claim 7, further comprising:

using a key indicator for indicating a used ciphering key and the integrity key used for generating the integrity check value, wherein the key indicator is concatenated to a value obtained by encryption of the subscriber identifying value.

9. (Original) The method according to claim 7, wherein the pseudo random function is a keyed hash function.

10. (Original) The method according to claim 7, wherein a calculated result of performing the pseudo random function is truncated to a predetermined amount of bits.

11. (Original) The method according to claim 1, wherein the subscriber identifying value is an International Mobile Subscriber Identity.

12. (Withdrawn) A method for validating a subscriber identifier, wherein the subscriber identifier comprises a format including at least integrity check values, the method comprising the steps of:

detecting an integrity check value of a received subscriber identifier,

performing an integrity check based on the integrity check value and the subscriber identifier, and

rejecting the subscriber identifier in case the integrity check reveals that the subscriber identifier is not valid.

13. (Withdrawn) The method according to claim 12, further comprising the step of

decrypting the subscriber identifier in case the integrity check is successful.

14. (Currently Amended) An apparatus ~~network control node~~ for generating a subscriber identifier, the network node comprising:

means for generating an identifier base string based on encrypting a subscriber identifying value;

means for generating an integrity check value based on the identifier base string; and

means for generating the subscriber identifier based on a concatenation of the identifier base string and the integrity check value.

wherein the means for generating the identifier base string comprises:

means for binary coding of the subscriber identifying value;

means for concatenating a random number to the binary coded subscriber identifying value; and

means for performing an encryption algorithm on the concatenated binary coded subscriber identifying value and random number for generating the identifier base string.

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) The ~~network control node~~apparatus according to claim 14, wherein the means for generating the subscriber identifier is further for concatenating ~~subscriber identifier generating means is adapted to concatenate~~ a key indicator~~,~~ and is further for indicating a used ciphering key~~,~~ to a value obtained by the encryption of the subscriber identifying value.

18. (Currently Amended) The ~~network control node~~apparatus according to claim 14, wherein the means for generating the subscriber identifier is further for concatenating ~~subscriber identifier generating means is adapted to concatenate~~ an

identifier type indicator~~,~~ and is further for indicating that the subscriber identifier is a particular identifier type~~,~~ to a value obtained by the encryption of the subscriber identifying value.

19. (Currently Amended) The ~~network control node~~apparatus according to claim ~~15~~14, wherein a defined length is provided for the concatenated binary coded subscriber identifying value and the random number, and wherein the means for performing the encryption algorithm is further for ~~encryption algorithm performing means is adapted to~~ setting a value of one for the most significant bits not used for the binary coded subscriber identifying value.

20. (Currently Amended) The ~~network control node~~apparatus according to claim 14, wherein the means for generating an integrity check value is further for ~~integrity check value generating means is adapted to~~ performing a pseudo random function on the identifier base string using an integrity key.

21. (Currently Amended) The ~~network control node~~apparatus according to claim 14, wherein the means for generating the subscriber identifier is further for concatenating ~~subscriber identifier generating means is adapted to concatenate~~ a key indicator for indicating a used ciphering key and an integrity key used for generating the

integrity check value to a value obtained by the encryption of the subscriber identifying value.

22. (Currently Amended) The ~~network control node~~apparatus according to claim 20, wherein the pseudo random function is a keyed hash function.

23. (Currently Amended) The ~~network control node~~apparatus according to claim 20, wherein the means for generating an integrity check value is further for truncating ~~integrity check value generating means is adapted to truncate~~ a calculated result of the pseudo random function to a predetermined amount of bits.

24. (Currently Amended) The ~~network control node~~apparatus according to claim 14, wherein the subscriber identifying value is an International Mobile Subscriber Identity.

25. (Withdrawn) A network control node for validating a subscriber identifier, wherein the subscriber identifier comprises a format including at least integrity check values, the network control node comprising:

means for detecting an integrity check value of a received subscriber identifier:

means for performing an integrity check based on the integrity check value and the subscriber identifier; and

means for rejecting the subscriber identifier in case the integrity check reveals that the subscriber identifier is not valid.

26. (Withdrawn) The network control node according to claim 25, further comprising means for decrypting the subscriber identifier in case the integrity check is successful.

27. (Withdrawn) The network control node according to claim 25, wherein the network control node comprises an AAA (Authentication, Authorization, and Accounting) server.

28. (Currently Amended) A computer program product stored on a tangible medium, the product comprising software code, when executed by one or more processors, performs:

generating an identifier base string based on encrypting a subscriber identifying value;

generating an integrity check value based on the identifier base string; and generating a subscriber identifier based on a concatenation of the identifier base string and an integrity check value,

wherein the generating the identifier base string comprises:

binary coding of the subscriber identifying value,

concatenating a random number, and

performing an encryption algorithm on the concatenated binary coded subscriber identifying value and the random number for generating the identifier base string.

29. (Original) The computer program product according to claim 28, wherein the computer program product comprises distributed components stored in more than one location of a network.

30. (Original) The computer program product according to claim 28, wherein said computer program product is directly loadable into the internal memory of a computer.

31. (Original) The computer program product according to claim 28, wherein the computer program product comprises a computer-readable medium on which said software code is stored.